UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/779,950	02/13/2004	Sanjay Kaniyar	13768.491	9155

22913 7590 07/18/2008

WORKMAN NYDEGGER
60 EAST SOUTH TEMPLE
1000 EAGLE GATE TOWER
SALT LAKE CITY, UT 84111

EXAMINER	
MCNALLY, MICHAEL S	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
07/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/779,950	KANIYAR ET AL.	
	Examiner	Art Unit	
	Michael S. McNally	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 May 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9,10,21-27,29 and 30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9,10,21-27,29 and 30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Detailed Action

Status of Claims:

Claims 1-40 are pending in this Office Action.

Claims 1, 2, 5, 9, 21, 22, 25 and 29 are amended.

Claims 8, 11-20, 28 and 31-40 are cancelled.

The claims and only the claims form the metes and bounds of the invention. "Office personnel are to give claims their broadest reasonable interpretation in light of the supporting disclosure. In re Morris, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim are not read into the claim. In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA 1969)" (MPEP p 2100-8, c 2, l 45-48; p 2100-9, c 1, l 1-4). The Examiner has full latitude to interpret each claim in the broadest reasonable sense. The Examiner will reference prior art using terminology familiar to one of ordinary skill in the art. Such an approach is broad in concept and can be either explicit or implicit in meaning.

Applicant's Remarks indicate the status of claim 8 as pending. In Applicant's amended claims, however, claim 8 has been cancelled and is being treated as such.

Response to Arguments

Applicant's arguments filed in the amendment filed 13 May 2008, have been fully considered but they are not persuasive. The reasons are set forth below.

Applicant's invention as claimed:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2, 4-7, 10, 21-22, 24-28 and 30 are rejected under 35 U.S.C. 102(b) as being anticipated by Network working Groups, request for Comments 1948, "Defending against Sequence Number Attacks" by *Bellovin*.

As to **claims 1 and 21**, *Bellovin* teaches: In a local server that receives data from one or more remote clients over a data transport protocol (*Bellovin:* Page 2, Lines 1-5; client talking to server using a TCP connection), a method/computer program product of generating an initial sequence number for use by a remote client when assigning sequence numbers to one or more data packets to be sent to the local server (*Bellovin*: Page 3, Lines 22-24), the initial sequence number generated in a manner that prevents the local server from being attacked while maintaining reliable data transfer (*Bellovin:* Page 4, Lines 1-3; Compute F in such a way that it cannot be guessed by discovering other initial sequence numbers), the method comprising the acts of:

generating a random input key using a secret maintained by the local server (*Bellovin*: Page 4, Lines 3-13; F value generated based on a per-host secret);

receiving a connection identifier key that includes connection information for at least the remote client (*Bellovin*: Page 3, Lines 37-38; 4-tupe of <localhost, localport, remotehost, remoteport> used to compute F);

securely initializing a hash function with at least a portion of the random input key and at least a portion of the connection identifier key for determining an intermediate value of (*Bellovin*: Page 4, Lines 3-5; F is a cryptographic hash of connection id and secret data, thus it is secure and contains the claimed data);

creating a monotonically increasing counter (*Bellovin*: Page 2, Lines 25-27, Counter M) for ensuring that a same connection identifier does not have data collisions from competing sequence numbers within a predetermined period of time (*Bellovin*: Page 3, Lines 23-25; prevent stale packets from being accepted by new incarnation f same connection), and for ensuring randomness of the initial sequence number on a per connection basis for preventing attacks on the local server (*Bellovin*: Page 2, Lines 25-32, insufficient randomness leads to attacks), the counter taking both timer information and connection rate information as input (*Bellovin:*Page 2, Lines 25-33; counter incremented by a constant every second and by a value per connection);

incrementing the counter a fixed value based on a passage of a predetermined time period (*Bellovin*: Page 2, Lines 26-30, M incremented either 1 every 4 microsecond in one implementation or by a constant per second in another);

detecting a connection rate for the local server (Bellovin: Page 2, Lines 28-30; counter is incremented on a per connection basis, accordingly, the connection rate is known)

incrementing the counter a variable amount depending upon a rate of connections with the local server, the increment being based upon the connection rate (*Bellovin:* Page 2, Lines 28-30; under Berkeley implementation, the counter is implemented by a constant for every connection. The rate of connections is a variable amount so that even with a constant value for each connection, the increment is variable based on the rate of connections); and

combining the fixed value and the variable amount to create a random value (Bellovin: Page 2, Lines 28-30); and

combining the intermediate value and the random value using a monotonically increasing mathematical function to generate the initial sequence number (*Bellovin*: Page 3-4; ISN computed using M + F (localhost, localport, remotehost, remoteport), where M = fixed + variable from above and F is the intermediate value from the 4-tuple as calculated above; M+F is a strictly increasing function)

As to **claims 2 and 22**, *Bellovin* further teaches wherein if the connection rate is below the threshold value, the fixed value is further incremented based on each connection established with the local server (*Bellovin*: Page 2, Lines 25-32).

As to **claims 4 and 24**, *Bellovin* further teaches wherein the connection identifier key further includes connection information for one or more of the local server port, local server routing address, remote port and remote routing address (*Bellovin*: Page 3, Lines 37-38; 4-tuple of <localhost, localport, remotehost, remoteport> used to compute F).

As to **claims 5 and 25**, *Bellovin* further teaches wherein the data transport protocol is Transmission Control Protocol (TCP) (*Bellovin*: Page 2, Lines 1-3), and

wherein the local and remote routing addresses are Internet Protocol (IP) addresses (*Bellovin*: Page 4, Lines 9, 16).

As to **claims 6 and 26**, *Bellovin* further teaches wherein at least a second connection is made between the local server and a second remote client (*Bellovin*: Page 3, Lines 35-42), and wherein the method further including the acts of:

receiving a second connection identifier key that includes connection information for at least the second remote client (*Bellovin*: Page 3, Lines 35-42);

securely initializing the hash function with at least a portion of the random input key and at least a portion of the second connection identifier key for determining a second intermediate value of a second initial sequence number (*Bellovin*: Page 4, Lines 3-5; F is a hash of connection id and secret data);

based on at least a portion of the second connection identifier key (*Bellovin*: Page 3, Lines 35-42, each 4-tuple gets its own number space), creating a second monotonically increasing counter (*Bellovin*: Page 2, Lines 25-27, Counter M) for ensuring that a same connection identifier does not have data collisions from competing sequence numbers within a predetermined period of time (*Bellovin*: Page 3, Lines 23-25; prevent stale packets from being accepted by new incarnation f same connection), and for ensuring randomness of the initial sequence number on a per connection basis for preventing attacks on the local server (*Bellovin*: Page 2, Lines 25-32, insufficient randomness leads to attacks);

incrementing the second counter the fixed value based on the passage of the predetermined time period (*Bellovin*: Page 2, Lines 26-30, M incremented either 1 every 4 microsecond in one implementation or by a constant per second in another);

incrementing the second counter a second variable amount depending upon a rate of connections with the local server and for those connections associated with the second counter, wherein if the rate of connections with the local server and for those connections associated with the second counter is beyond a threshold value the variable increment is based on an elapsed time, otherwise the variable increment is based on each connection established with the local server and associated with the second counter (*Bellovin:* Page 2, Lines 28-30; under Berkeley implementation, the counter is implemented by a constant for every connection. The threshold value for Berkeley would be when the rate of the number of connections cannot increase due to system considerations, at that point the counter would be applied on an elapsed time, i.e. How long it takes to establish a connection, rather than on a per connection basis); and

combining the second intermediate value, the fixed value and the second variable amount for generating the second initial sequence number (*Bellovin*: Page 3-4; ISN computed using M + F(localhost, localport, remotehost, remoteport), where M = fixed + variable from above and F is the intermediate value from the 4-tuple as calculated above).

As to **claims 7 and 27**, *Bellovin* further teaches wherein the arbitrary information maintained as a secret by the local server is based on timing, state conditions for the

local server, or both, at boot up time of the local server, which include one or more of a time of day, a day of month, a month, a year, a local server hard drive head position, and whether input was detected by hardware of the local server (*Bellovin*: Page 4, Lines 7-9; Boot time of the machine used in secret data, which necessarily includes at least one of the time of day, month or year if not all).

As to **claims 10 and 30**, *Bellovin* further teaches , wherein the monotonically increasing counter is shared by at least two connections at the same time (*Bellovin*: Page 2, Lines 28-30, counter used by all connections to server, as each new connection increments it).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Network working Groups, request for Comments 1948, "Defending against Sequence Number Attacks" by *Bellovin* in view of U.S. Patent Application Publication No. 2002/0187788 to *McKay*.

As to **claim 3**, *Bellovin* discloses all recited limitations of claim 1 from which claim 3 depends.

Bellovin does not expressly disclose wherein based on the fixed value, if a remote client's data transfer rate while connected to the local server is less than a specified byte rate then the connection identifier used by the remote client the is allowed immediate re-connection to the local server after the remote client disconnects.

McKay discloses wherein based on the fixed value, if a remote client's data transfer rate while connected to the local server is less than a specified byte rate then the connection identifier used by the remote client the is allowed immediate re-connection to the local server after the remote client disconnects (*McKay*: Fig 6; Page 1, Sec 7 and Page 3-4, Sec 27-33; when service degrades below and acceptable level and the user is disconnected, the connection is re-established).

Bellovin and *McKay* are analogous art because they are from the art of networks.

At the time of invention, it would have been obvious to a person of ordinary skill in the art to allow connections without the possibility of collision the ability to reconnect. The rationale would have been to reduce network disruptions (*McKay*: Page 1, Sec 2)

4. Claims 9 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Network working Groups, request for Comments 1948, "Defending against Sequence Number Attacks" by *Bellovin* in view of U.S. Patent Application Publication No. 2002/0083175 to *Afek et al.*

As to **claims 9 and 29**, *Bellovin* discloses all recited limitations of claims 1, 11, 20 and 30 from which claims 9, 19, 29 and 39 depend respectively. *Bellovin* additionally discloses wherein if the connection rate is beyond the threshold value the variable increments up to an amount of 0x000022FB every millisecond (*Bellovin:* Page 2, Lines 26-30),

Bellovin does not expressly disclose otherwise the variable increment is an amount between 16 K and 32 K.

Afek discloses otherwise the variable increment is an amount between 16 K and 32 K (Afek, Fig 4B).

Bellovin and *McKay* are analogous art because they are from the art of networks.

At the time of invention, it would have been obvious to use variable increments depending on threshold values. The rationale would have been that it is obvious to combine these known elements to yield the predictable result of the instant application. *Bellovin* and *Afek* in combination contained all of the elements required for claims 9, 19, 29 and 39, however, the difference being that neither *Bellovin* nor *Afek* combined said elements. One of ordinary skill in the art could have combined the elements present in *Belovin* and *Afek* with the knowledge that in combination, said elements would have performed the same functions that they did separately. Furthermore, one of ordinary

skill in the art would have recognized that the results of the combination were predictable. In fact, for one of ordinary skill in the art of software systems development, there would have been a reliance on the fact that the results of the combination would be predictable.

5. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Network working Groups, request for Comments 1948, "Defending against Sequence Number Attacks" by *Bellovin* in view of U.S. Patent Application Publication No. 2002/0187788 to *McKay* and U.S. Patent No. 3,728,535 to *Dickman et al.*

As to **claim 23**, *Bellovin* discloses all recited limitations of claims 21 from which claim 23 depends.

Bellovin does not expressly wherein the fixed value is 25.6 K (*Dickman*: Col 7, Line 8), and wherein if a remote client's data transfer rate while connected to the local server is less than 256 K then the connection identifier used by the remote client the is allowed immediate re-connection to the local server after the remote client disconnects (*McKay*: Fig 6; Page 1, Sec 7 and Page 3-4, Sec 27-33).

Dickman discloses wherein the fixed value is 25.6 K (*Dickman*: Col 7, Line 8).

McKay discloses wherein if a remote client's data transfer rate while connected to the local server is less than 256 K then the connection identifier used by the remote client the is allowed immediate re-connection to the local server after the remote client disconnects (*McKay*: Fig 6; Page 1, Sec 7 and Page 3-4, Sec 27-33).

Bellovin, *McKay* and *Dickman* are analogous art because they are from the art of networks.

At the time of invention, it would have been obvious to a person of ordinary skill in the art to allow connections operating at various connection speeds without the possibility of collision the ability to reconnect. The rationale would have been to reduce network disruptions (*McKay*: Page 1, Sec 2).

REMARKS

Applicant has presented amendments the independent claims. The examiner maintains the rejections, see remarks below.

The Applicant Argues:

Applicant argues that *Bellovin* fails to teach securely initializing a hash function with at least a portion of the random input key and at least a portion of the connection identifier key for determining an intermediate value.

In response, the examiner respectfully submits:

Bellovin teaches the disclosed limitation at Lines 1-5 of Page 4. F (the function) is securely computed as a cryptographic hash function and uses the connection id and secret data (which corresponds to the random input key).

Applicant argues that Bellovin also fails to teach creating a monotonically increasing counter for ensuring that a same connection identifier does not have data collisions from competing sequence numbers within a predetermined period of time, and

for ensuring randomness of the initial sequence number on a per connection basis for preventing attacks on the local server, the counter taking both timer information and connection rate information as input.

In response, the examiner respectfully submits:

Bellovin teaches the disclosed limitation at Pages 2 and 3 as described above in the rejection of claim 1.

Applicant argues that Bellovin also fails to teach incrementing the counter a fixed value based on a passage of a predetermined time period and detecting a connection rate for a local server.

In response, the examiner respectfully submits:

Bellovin teaches the disclosed limitation at page 2, Lines 26 -30. Bellovin clearly describes incrementing the counter a constant per time period (a constant value each second) as well as detecting incoming connections and incrementing the counter on that basis.

Applicant argues that Bellovin also fails to teach incrementing the counter a variable amount depending upon the connection rate for local server, the increment being based upon the connection rate and combining the fixed value and the variable amount to create a random value.

In response, the examiner respectfully submits:

Bellovin teaches the disclosed limitation at Pages 2-4 in relevant part as described in the rejection of claim 1 above.

Applicant argues that Bellovin also fails to teach combining the intermediate value and the random value using a monotonically increasing mathematical function to generate the initial sequence number.

In response, the examiner respectfully submits:

Bellovin teaches the disclosed limitation at Pages 3-4 as described in the rejection of claim 1 above.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael S. McNally whose telephone number is (571)270-1599. The examiner can normally be reached on Monday through Friday 9:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MSM
17 July 2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136